

ELLIPTIC CURVES OF ALMOST-PRIME CONDUCTOR

SEAN HOWE AND KIRTI JOSHI

Draft of 2012-01-22

ABSTRACT. We use elementary techniques to study elliptic curves over \mathbb{Q} of conductor N equal to the product of two distinct odd primes. Using a result of Iwaniec on the representation of almost-primes by quadratic forms, we show that infinitely many N equal to a prime or the product of two distinct odd primes arise as the conductors of elliptic curves over \mathbb{Q} . Inspired by earlier work in the case of prime conductor, we also provide a non-existence result: We show that there are no elliptic curves over \mathbb{Q} of conductor N when N is the product of two primes satisfying certain congruency and quadratic class number conditions. We use a computer to find all 67 values of $N < 10^7$ satisfying these conditions.

Sean Howe, Math. Inst., Universiteit Leiden, 2300 RA Leiden, The Netherlands
seanpkh@gmail.com

Kirti Joshi, Math Dept., University of Arizona, 85719 Tucson, Arizona, USA
kirti@math.arizona.edu

CONTENTS

1. Introduction	1
2. Existence results	2
3. Non-existence results	4
4. Tables	8
References	10

1. INTRODUCTION

In this paper we use elementary techniques to study elliptic curves over \mathbb{Q} of conductor N equal to the product of two distinct odd primes. The primary aim of this work was to find infinitely many elliptic curves over \mathbb{Q} with conductors having a small number of prime factors. Although we were unable to prove the existence of an infinite family of curves of differing prime conductor, we were able to construct families containing infinitely many curves having different conductors equal to the product of at most two distinct primes. This is the contents of our first main result, Theorem 1. In our second main result, Theorem 7, we provide a non-existence result that applies to certain conductors of this form.

While elliptic curves of prime conductor were studied extensively in the 1960s and 70s using the techniques of basic class field theory and diophantine analysis (see the classic work of Neumann [8], Ogg [9, 10], Setzer [12], and Brumer and Kramer [2, Sec. 5 and 6]), with the exception of Hadano's [4] work on conductors of the form $2^m p$, to the best of our knowledge these techniques have not been extended to

any more general conductor N . In Section 3 we employ techniques similar to this classical work in order to show that there are no elliptic curves of conductor $N = pq$ for p and q odd primes satisfying certain congruency and quadratic class number conditions (Theorem 7). Taking advantage of modern computing power we find all 67 values of $N < 10^7$ satisfying these conditions (Table 2), giving many examples of large N of this form such that there are no elliptic curves over \mathbb{Q} of conductor N , most of which are not contained in John Cremona's tables of elliptic curve data [3]. Furthermore, by considering conductor equal to the product of two primes instead of just a single prime we are also able to provide an infinite existence result: in Section 2 (Theorem 1 and Corollary 3) we show that there infinitely many natural numbers N equal to either a prime or the product of two distinct odd primes such that there exists an elliptic curve over \mathbb{Q} of conductor N .

Acknowledgements. This work grew out of the first author's undergraduate thesis at the University of Arizona, advised by the second author. We would like to thank Bas Edixhoven and Jaap Top for their help and encouragement in bringing this work to its current state. The first author was supported by an Erasmus Mundus scholarship and enrolled in the ALGANT integrated master course during part of the preparation of this paper.

2. EXISTENCE RESULTS

In Theorem 1, the main result of this section, we produce families of elliptic curves such that in each of these families infinitely many natural numbers N equal to a prime or the product of two distinct odd primes arise as conductors:

Theorem 1. *Let $a, b \in \mathbb{Z}$ be such that at least one of a and b is not divisible by 3 and such that*

$$a^{12} - 9a^8b + 27a^4b^2 - 27b^3$$

is not a square. Then there exist infinitely many $n \in \mathbb{Z}$ such that the Weierstrass equation

$$(2.1) \quad y^2 + y = x^3 + ax^2 + bx + n$$

has discriminant of the form $\Delta(n) = -pq$ for p an odd prime and q either 1 or an odd prime distinct from p . In particular, for such a value of n this equation gives a global minimal model of an elliptic curve with conductor $N = pq$, and there are infinitely many natural numbers N of this form arising as conductors of curves in this family.

Proof. The elliptic curve E defined by Equation 2.1 has discriminant

$$\Delta(n) = (-432)n^2 + (-64a^6 + 288a^2b - 216)n + (-16a^6 + 16a^4b^2 - 64b^3 + 72a^2b - 27).$$

In particular, considering this as a quadratic polynomial in n , the leading coefficient -432 is divisible only by 2 and 3, but the constant coefficient is odd and by our condition on $a, b \pmod{3}$ either the coefficient of n or the constant coefficient is not divisible by 3, thus the gcd of the coefficients is 1. Furthermore, a calculation shows that if we consider $\Delta(n)$ as a quadratic polynomial in n then its discriminant is equal to

$$2^{12} \cdot (a^{12} - 9a^8b + 27a^4b^2 - 27b^3)$$

which by hypothesis is not square and thus $\Delta(n)$ is an irreducible polynomial in n .

Thus, by Iwaniec's theorem on quadratic forms (stated below as Theorem 2), there are infinitely many integers n such that the quadratic form inside the parentheses takes on a value with at most 2 prime factors. Since $\Delta(n) \equiv 5 \pmod{8}$, these values are never plus or minus a square, thus at these n

$$\Delta(n) = \pm pq,$$

where p is an odd prime and $q \neq p$ is either 1 or an odd prime. Fix such an n . Because every prime appears in $\Delta(n)$ with exponent less than 12, this must be a minimal discriminant at all primes and thus Equation 2.1 is a global minimal Weierstrass equation.

Recall that an elliptic curve has good reduction at a prime if and only if that prime does not divide the minimal discriminant and multiplicative reduction at a prime if and only if that prime divides the minimal discriminant but not the quantity c_4 associated to a minimal Weierstrass equation [13, Prop. 5.1]. In particular, since $1728\Delta = c_4^3 - c_6^2$, any prime other than 2 or 3 dividing Δ and c_4 (and thus having additive reduction) divides Δ to a power higher than 1. Since $\Delta(n)$ is odd, neither p nor q is 2, and since no prime divides $\Delta(n)$ to a power higher than 1, any p or q not equal to 3 has multiplicative reduction. However, for Equation 2.1,

$$c_4 = 16a^4 - 48b$$

which is divisible by 3 if and only if a is. But if $a \equiv 0 \pmod{3}$, then $\Delta(n) \equiv 2b^3 \pmod{3}$ and since not both a and b are divisible by 3, $\Delta(n)$ is not divisible by 3. Thus if p or q is 3 the curve still has multiplicative reduction and we conclude that the conductor is exactly $N = pq$.

Finally, the formula for $\Delta(n)$ shows that the infinitely many n given by Iwaniec's theorem give rise to infinitely many distinct discriminants, from which we deduce the final statement of the theorem. \square

In the proof of the above we made use of the following theorem of Iwaniec [6, Sec. 1]:

Theorem 2 (Iwaniec [6, Sec. 1]). *Let $G(x) = ax^2 + bx + c$ be an irreducible polynomial over \mathbb{Z} . If $a > 0$ and $c \equiv 1 \pmod{2}$ then there are infinitely many $n \in \mathbb{Z}$ such that $G(n)$ has at most two prime factors (counted with multiplicity).*

Note that Iwaniec also provides an estimate on the number of such n . The following is a straightforward corollary of Theorem 1:

Corollary 3. *There are infinitely many natural numbers N equal to either a prime or the product of two distinct odd primes such that there exists an elliptic curve over \mathbb{Q} with conductor N .*

Remark. In the proof of Theorem 1 we observed that the discriminant $\Delta(n)$ is always congruent to 5 mod 8 for the curves produced. This shows that p and q are never both congruent to $\pm 1 \pmod{8}$, giving an obvious separation from the primes appearing in our nonexistence results later on which will all be congruent to $\pm 1 \pmod{8}$. We also note that the condition that one of a and b not be divisible by 3 is necessary for our method since otherwise $\Delta(n) \equiv 0 \pmod{3}$. In Table 1 we calculate the prime or almost prime $N < 1000$ appearing as conductors of curves in the families of Theorem 1 for $|a|, |b|, |n| < 100$.

Remark. The condition that $a^{12} - 9a^8b + 27a^4b^2 - 27b^3$ not be square is satisfied, for instance, if b is much larger than $|a|$ so that the quantity is negative, or if $(a, b) \bmod 8$ is one of $(0, 1), (0, 3), (0, 7), (1, 2), (1, 4), (1, 6), (2, 1), (2, 3), (2, 7), (3, 2), (3, 4), (3, 6), (4, 1), (4, 3), (4, 7), (5, 2), (5, 4), (5, 6), (6, 1), (6, 3), (6, 7), (7, 2), (7, 4)$, or $(7, 6)$. For a fixed generic value of b (resp. a) the curve

$$y^2 = a^{12} - 9a^8b + 27a^4b^2 - 27b^3$$

has genus greater than 0, thus by Siegel's theorem there will be at most finitely many integer values of a (resp. b) such that this quantity is a square.

Remark. A well-known conjecture of Hardy and Littlewood on quadratic polynomials (see [5] for the original conjecture or [1] for a more recent survey) implies that for any of the families to which Theorem 1 applies there are infinitely many values of n giving prime conductor (i.e. such that $\Delta(n)$ has one prime factor). Concretely, the conjecture says that

$$p(x) \sim C \cdot \frac{\sqrt{x}}{\log x}$$

where $p(x)$ is the number of positive $n \leq x$ such that $\Delta(n)$ has a single prime factor and gives a formula for the constant C , which in our case will depend on a and b . For example, when $a = b = 1$ our theorem applies,

$$\Delta(n) = -432n^2 + 8n - 19,$$

and we calculate $C \sim 0.063$. When $a = 0, b = 1, C \sim 0.162$.

Remark. Setzer [12, Thm. 2] showed that for $p \neq 2, 3, 17$ there is an elliptic curve of conductor p with a rational 2-torsion point if and only if $p = u^2 + 64$ for some integer value of u . It is not known whether or not there are infinitely many primes of this form, and because 64 is not odd we cannot apply Iwaniec's theorem to say that there are at least infinitely many almost primes of this form.

3. NON-EXISTENCE RESULTS

Following the approach of Setzer [12] for prime conductor, we first show that under certain class number conditions an elliptic curve of conductor N equal to a product of distinct primes must have a rational point of order 2 (Theorem 4). We then use the existence of such a point in the special case where N is the product of two odd primes in order to construct a solution of a Diophantine equation (Theorem 5), and then give conditions under which these Diophantine equations have no solution (Proposition 6). We conclude by combining these results in order to show that under certain class number and congruency conditions on primes p and q there can be no elliptic curve of conductor $N = pq$ (Theorem 7) and in Table 2 we list all 67 values of $N = pq < 10^7$ to which this result applies.

3.1. Forcing a rational point of order 2.

Theorem 4. *Let $N = p_1 \dots p_n$ be a product of distinct primes such that either $p_i = 2$ for some i or $p_i \equiv \pm 1 \pmod{8}$ for all $1 \leq i \leq n$ and suppose that for any $m = \pm p_{i_1} \dots p_{i_l}$, $1 \leq i_1 < i_2 < \dots < i_l \leq n$ the class number of $\mathbb{Q}(\sqrt{m})$ is not divisible by 3. Then any elliptic curve over \mathbb{Q} of conductor N has a rational point of order 2.*

Proof. Let E be an elliptic curve over \mathbb{Q} of conductor N with minimal discriminant Δ . Suppose E has no rational point of order 2. It then follows from a result of Brumer and Kramer [2, Cor. 5.3] that $\mathbb{Q}(\sqrt{\Delta})$ has class number divisible by 3 (the only subtlety in applying their result comes when all the p_i are odd, in which case one must make the observation that Δ , as plus or minus a product of these p_i to some powers, cannot be congruent to 5 mod 8 and thus E is not supersingular at 2 by part (2) of the cited corollary). However, the field $\mathbb{Q}(\sqrt{\Delta})$ is equal to a field of the form $\mathbb{Q}(\sqrt{m})$ for $m = \pm p_{i_1} \dots p_{i_l}$, $1 \leq i_1 < i_2 < \dots < i_l \leq n$ or $m = \pm 1$, and thus we obtain a contradiction since by our hypothesis (or by standard result for $m = \pm 1$) the class number of this field is not divisible by 3. \square

Remark. The result of Brumer and Kramer cited in the proof of Theorem 4 is a corollary of Serre's [11] detailed description of the Galois action on torsion points of a semi-stable elliptic curve over \mathbb{Q} , from which Brumer and Kramer also derive many more interesting results about the two and three torsion of semi-stable curves. We should note, however, that it is also possible to give a simple direct proof of Theorem 4 using only basic class field theory to analyze the two-torsion field. A proof along these lines is a straightforward generalization of the work of Ogg [9, 10] and Setzer [12] in the case of prime conductor, and thus we omit it here.

3.2. Diophantine analysis of curves with a rational point of order 2. Our first step is to develop a list of Diophantine equations (Theorem 5), one of which must have a solution if there exists a curve of conductor $N = pq$ with a rational point of order 2. In Proposition 6 we use this list to show that under certain congruency conditions on p and q no curve with conductor $N = pq$ can have a rational point of order 2.

Suppose that E is an elliptic curve with conductor $N = pq$ for distinct odd primes p and q and also that E has a rational point of order 2. Following Setzer [12, Sec. 2], we obtain an integral solution (A, B, α, β) to the following:

$$\begin{aligned} B^2(A^2 - 4B) &= \pm 2^8 p^\alpha q^\beta, \text{ where:} \\ 1 &\leq \alpha, \beta \\ p \text{ and } q &\text{ each divide at most one of } A, B, \\ \text{one of the following holds} &- \begin{aligned} &A \equiv 1 \pmod{4} \text{ and } B \equiv 0 \pmod{16} \text{ or} \\ &A \equiv 6 \pmod{8} \text{ and } B \equiv 1 \pmod{8} \end{aligned} \end{aligned}$$

In particular, taking into account the congruency conditions and the fact that each of p and q divide at most one of A and B , we see that the only possible values of B are 1, ± 16 , $\pm p^{\alpha/2}$ (when α is even and this is congruent to 1 mod 8), $\pm q^{\beta/2}$ (when β is even and this is congruent to 1 mod 8), $\pm 16p^{\alpha/2}$ (when α is even), $\pm 16q^{\beta/2}$ (when β is even), $\pm p^{\alpha/2}q^{\beta/2}$ (when α and β are even and this is congruent to 1 mod 8), and $\pm 16p^{\alpha/2}q^{\beta/2}$ (when α and β are even). We analyze these cases:

- If $B = 1$ then $A^2 - 4 = \pm 256p^\alpha q^\beta$. When the righthand side is negative there is no solution. When the righthand side is positive, letting $C = A - 2$,

$$C(C + 4) = 256p^\alpha q^\beta$$

and since the only prime that can divide both C and $C + 4$ is 2 and $C \equiv 4 \pmod{8}$ we see $C = 2^2 p^\alpha$ and $C + 4 = 2^6 q^\beta$, possibly after swapping p and q . Thus $4 = 2^6 q^\beta - 2^2 p^\alpha$, so we obtain either $1 = 2^4 q^\beta - p^\alpha$ or $1 = 2^4 p^\alpha - q^\beta$.

- If $B = 16$ then $A^2 - 64 = \pm p^\alpha q^\beta$. If the righthand side is negative then, up to swapping p and q , we obtain the finitely many solutions (remembering the congruency conditions on A and that p and q are odd)

$$(A, p^\alpha, q^\beta) \in \{(1, 3^2, 7), (-3, 5, 11), (5, 3, 13), (-7, 3, 5)\}.$$

If the righthand side is positive then $(A - 8)(A + 8) = p^\alpha q^\beta$ and since the only prime that can divide both $A - 8$ and $A + 8$ is 2, we conclude $|p^\alpha - q^\beta| = 16$.

- If $B = -16$ then $A^2 + 64 = \pm p^\alpha q^\beta$. If the righthand side is negative then there are no solutions.
- In the rest of the cases, we make no reductions.

In summary, we have shown:

Theorem 5. *If there is an elliptic curve over \mathbb{Q} of conductor $N = pq$ with a rational point of order 2 for p and q odd primes, and N is not 15, 21, 39, or 55, then, up to swapping p and q , one of the following diophantine equations has an integral solution (A, a, b) with $a, b > 0$:*

Equations

-
- (1) $1 = 2^4 q^b - p^a$
 - (2) $|p^a - q^b| = 16$
 - (3) $A^2 + 64 = p^a q^b$
 - (4) $A^2 \pm 64 q^b = \pm p^a$
 - (5) $A^2 \pm 4 q^b = \pm 256 p^a$ and $q^b \equiv \pm 1 \pmod{8}$, the sign being the opposite of that on $4 q^b$
 - (6) $A^2 \pm 4 p^a q^b = \pm 256$
 - (7) $A^2 \pm 64 p^a q^b = \pm 1$

Setzer [12, Thm. 2] uses a similar analysis to show that there exists an elliptic curve over \mathbb{Q} of prime conductor $N = p$, $p \neq 2, 3, 17$ with a rational point of order 2 if and only if there is a solution to $A^2 + 64 = p$, the analogous condition to the third equation in our Theorem 5. Although the situation is less exact in the case of two primes, we can still give sufficient conditions on p and q for none of these equations to have a solution:

Proposition 6. *Suppose p and q are distinct primes such that $p, q \equiv 31 \pmod{60}$ but $p \notin \langle q \rangle$ where $\langle q \rangle$ is the subgroup generated by q in $(\mathbb{Z}/16\mathbb{Z})^\times$. Then there is no elliptic curve of conductor $N = pq$ with a rational point of order 2.*

Proof. By Theorem 5 it suffices to show that there is no solution to any of the diophantine equations listed in the table therein (as well as those with the roles of p and q swapped)

From equation (1), we obtain $1 \equiv 0 \pmod{3}$, a contradiction.

From equation (2), we obtain $p^a \equiv q^b \pmod{16}$. With our conditions on p and q modulo 16, a simple analysis shows this can only happen when a and b are both even. If $p^a > q^b$ then

$$q^b = p^a - 16 = (p^{a/2} - 4)(p^{a/2} + 4)$$

but the only prime that can divide both $p^{a/2}-4$ and $p^{a/2}+4$ is 2 and thus $p^{a/2}-4 = 1$ and $p^{a/2} + 4 = q^b$, and thus $p = 5$, a contradiction to $p \equiv 1 \pmod{5}$. We obtain a similar contradiction if $q^b > p^a$.

From equation (3), we obtain

$$(A + 8i)(A - 8i) = p^\alpha q^\beta$$

but since $p, q \equiv 3 \pmod{4}$ they are prime in $\mathbb{Z}[i]$ and thus since neither can divide both $A + 8i$ and $A - 8i$ (they do not divide $16i$), both $A + 8i$ and $A - 8i$ are equal to rational integers times a unit in $\mathbb{Z}[i]$, but A is a rational integer so this cannot be the case.

Under our conditions, the equations in (4), (5), (6), and (7) all reduce mod 3 and mod 5 to:

$$\begin{aligned} A^2 \pm 1 &\equiv \pm 1 \pmod{3} \\ A^2 \pm (-1) &\equiv \pm 1 \pmod{5} \end{aligned}$$

If both signs are positive then any solution gives that 2 is a square mod 5, a contradiction. If both signs are negative, a solution gives that 3 is a square mod 5, again a contradiction. If the first sign is negative and the second is positive, then a solution gives that 2 is a square mod 3, a contradiction. Finally if the first sign is positive and the second is negative, then in all cases a solution gives a positive number equal to a negative number, again a contradiction. \square

3.3. Results.

Theorem 7. *Suppose p and q are distinct primes such that $p \equiv 7 \pmod{16}$, $q \equiv 15 \pmod{16}$, and $p, q \equiv 1 \pmod{15}$. Suppose furthermore that none of the class numbers of $\mathbb{Q}(\sqrt{\pm p})$, $\mathbb{Q}(\sqrt{\pm q})$, and $\mathbb{Q}(\sqrt{\pm pq})$ are divisible by 3. Then there are no elliptic curves of conductor pq .*

Proof. By Theorem 4, any such curve will have a rational point of order 2, but by Proposition 6 there is no such curve with a rational point of order 2. \square

In contrast to our existence result in Theorem 1, here we are not able to make an infinite non-existence statement because we cannot guarantee that there are infinitely many p and q satisfying the given class number conditions (we note that Kishi and Miyake [7] have given a characterization of quadratic fields with class number divisible by 3, but we were unsuccessful in adapting this classification to our purposes). Still, by running a simple exhaustive search Theorem 7 allows us to quickly compute many examples of large $N = pq$ such that there is no elliptic curve of conductor N . Table 2 lists all 67 of the $N = pq$ less than 10^7 to which Theorem 7 applies. In particular, we note that only three of these N are less than 210000 and thus the rest are not contained in Cremona's tables [3]. There are a total of 697 values of $N = pq$ less than 10^7 satisfying the congruency conditions of Theorem 7, and thus the class number conditions are satisfied about 1/10th of the time. It is interesting to note that among the 17 values of $N = pq$ less than 210000 satisfying the congruency conditions of Theorem 7, *none* of them occur as the conductors of elliptic curves (according to Cremona's tables; as noted above, our Theorem 7 applies to only three of them), however, this is probably insufficient to make any sort of conjecture. The source code for the SAGE program used to produce Table 2 is available by request to the authors.

4. TABLES

Table 1 lists the prime or almost prime $N < 1000$ appearing as conductors of curves in the families of Theorem 1 for $|a|, |b|, |n| < 100$. Table 2 lists the 67 values of $N = pq$ less than 10^7 to which Theorem 7 applies.

Table 1: All prime or almost prime conductors $N < 1000$ coming from families as in Theorem 1 with $|a| < 100, |b| < 100, |n| < 100$ and an equation giving rise to each.

Equation	N
$y^2 + y = x^3 - x^2 + x$	$N = 19$ (prime)
$y^2 + y = x^3 - x$	$N = 37$ (prime)
$y^2 + y = x^3 - 2x^2 - 7x - 31$	$N = 67$ (prime)
$y^2 + y = x^3 + x$	$N = 91 = 7 \cdot 13$
$y^2 + y = x^3 - 2x^2 - 2x - 85$	$N = 141 = 3 \cdot 47$
$y^2 + y = x^3 - 2x + 1$	$N = 163$ (prime)
$y^2 + y = x^3 - x - 1$	$N = 179$ (prime)
$y^2 + y = x^3 - 5x + 4$	$N = 197$ (prime)
$y^2 + y = x^3 - 2x - 1$	$N = 269$ (prime)
$y^2 + y = x^3 + x - 1$	$N = 307$ (prime)
$y^2 + y = x^3 - x^2 + 2x$	$N = 347$ (prime)
$y^2 + y = x^3 - x^2 - 2x - 2$	$N = 373$ (prime)
$y^2 + y = x^3 - 2x^2 + x - 7$	$N = 381 = 3 \cdot 127$
$y^2 + y = x^3 - x^2 - 2x$	$N = 389$ (prime)
$y^2 + y = x^3 - x^2 + x + 1$	$N = 443$ (prime)
$y^2 + y = x^3 - 4x + 3$	$N = 467$ (prime)
$y^2 + y = x^3 - 2x$	$N = 485 = 5 \cdot 97$
$y^2 + y = x^3 - 2x^2 + x$	$N = 571$ (prime)
$y^2 + y = x^3 - x + 1$	$N = 611 = 13 \cdot 47$
$y^2 + y = x^3 - 2x^2 + 2x - 5$	$N = 723 = 3 \cdot 241$
$y^2 + y = x^3 + x + 1$	$N = 739$ (prime)
$y^2 + y = x^3 + 2x - 1$	$N = 755 = 5 \cdot 151$
$y^2 + y = x^3 - 2x - 2$	$N = 811$ (prime)
$y^2 + y = x^3 - x^2 - 2x - 1$	$N = 813 = 3 \cdot 271$
$y^2 + y = x^3 - 10x + 12$	$N = 827$ (prime)
$y^2 + y = x^3 - 4x - 3$	$N = 829$ (prime)
$y^2 + y = x^3 - x^2 - 2x + 1$	$N = 899 = 29 \cdot 31$
$y^2 + y = x^3 - 5x^2 + 5x$	$N = 973 = 7 \cdot 139$

Table 2: The 67 values of $N = pq < 10^7$ such that Theorem 7 show there is no elliptic curve of conductor N .

N	p	q
40921	151	271
149641	151	991
171001	631	271
403321	151	2671
496201	1831	271

548281	151	3631
625321	631	991
626281	2311	271
691321	2551	271
693241	151	4591
928201	631	1471
951481	3511	271
1055641	151	6991
1454281	151	9631
1635481	151	10831
1671721	151	11071
1685401	631	2671
1814521	1831	991
1889161	151	12511
2179081	151	14431
2252281	8311	271
2432761	151	16111
2528041	2551	991
2650201	151	17551
2693401	1831	1471
3338761	151	22111
3479401	3511	991
3748201	13831	271
3752521	2551	1471
3943321	14551	271
4172281	151	27631
4317241	151	28591
4715881	151	31231
4890601	1831	2671
4906441	4951	991
5164681	3511	1471
5331961	151	35311
5730601	151	37951
5803081	151	38431
5925721	631	9391
6077161	631	9631
6095641	6151	991
6172681	2311	2671
6349801	23431	271
6414841	23671	271
6648361	1831	3631
6813721	2551	2671
6985801	631	11071
6999001	151	46351
7071481	151	46831
7390441	27271	271
7780681	28711	271
7832521	151	51871

8122441	151	53791
8235961	30391	271
8267401	151	54751
8406121	1831	4591
8412361	151	55711
8651641	631	13711
8774761	151	58111
9105961	631	14431
9262681	2551	3631
9341641	34471	271
9377881	3511	2671
9572041	151	63391
9666841	35671	271
9731881	35911	271

REFERENCES

- [1] Stephan Baier and Liangyi Zhao. On primes represented by quadratic polynomials. In *Anatomy of integers*, volume 46 of *CRM Proc. Lecture Notes*, pages 159–166. Amer. Math. Soc., Providence, RI, 2008.
- [2] Arnand Brumer and Kenneth Kramer. The rank of elliptic curves. *Duke Math. J.*, 44(4):715–743, 1977.
- [3] John Cremona. Elliptic curve data. <http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/>.
- [4] Toshihiro Hadano. On the conductor of an elliptic curve with a rational point of order 2. *Nagoya Math J.*, 53:199–210, 1974.
- [5] G. H. Hardy and J. E. Littlewood. Some problems of ‘Partitio numerorum’; III: On the expression of a number as a sum of primes. *Acta Math.*, 44(1):1–70, 1923.
- [6] Henryk Iwaniec. Almost-primes represented by quadratic polynomials. *Invent. Math.*, 47(2):171–188, 1978.
- [7] Yasuhiro Kishi and Katsuya Miyake. Parametrization of the quadratic fields whose class numbers are divisible by three. *J. Number Theory*, 80(2):209–217, 2000.
- [8] Olaf Neumann. Elliptische kurven mit vorgeschriebenem reduktionsverhalten. ii. *Math. Nachr.*, 56:269–280, 1973.
- [9] A. P. Ogg. Abelian curves of 2-power conductor. *Proc. Camb. Phil. Soc.*, 62:143–148, 1966.
- [10] A. P. Ogg. Abelian curves of small conductor. *J. reine und angew Math.*, 226:204–215, 1967.
- [11] J.-P. Serre. Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. *Invent. Math.*, 15:259–331, 1972.
- [12] Bennett Setzer. Elliptic curves of prime conductor. *J. London Math. Soc.*, 10:367–378, 1975.
- [13] Joseph Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.